REMARKS

Claims 1-6 and 8-27 are currently pending in the subject application and are presently under consideration. Claims 1, 6 and 18 have been amended as shown on pages 2-6 of the Reply. Claim 7 has been cancelled. In addition, claims 24-27 have been newly added.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-21 Under 35 U.S.C. §102(e)

Claims 1-23 stand rejected under 35 U.S.C. §102(e) as being anticipated by Maher, III *et al.* (US 2003/0118029 A1). Withdrawal of this rejection is requested for at least the following reasons. Maher, III *et al.* does not teach each and every element of the claimed subject matter as recited in the subject claims.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes ***each and every limitation*** set forth in the patent claim. *Trintec Industries, Inc. v. Top-U.S.A. Corp.,* 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). ***The identical invention must be shown in as complete detail as is contained in the ... claim.*** *Richardson v. Suzuki Motor Co.,* 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). (emphasis added).

The claimed subject matter relates to a network interface comprising an embedded network traffic analyzer. In particular, independent claim 1 recites *a system that facilitates analyzing a network, comprising: a network interface component that facilitates access to the network*, ***the network interface component comprising: a network traffic analyzer (NTA) component that analyzes network data and diagnoses network related data problems***. Maher does not teach or suggest the aforementioned novel aspects of applicants' claimed subject matter.

Maher provides a network device for enforcing service level agreements between service providers and customers. The network device includes memory, which contains information specific to each customer or subscriber. The memory is connected to a traffic flow scanning processor that scans each data packet flowing through the network device for header and payload information, associate each data packet with a particular subscriber and identifies the type and

nature of the network traffic. Once the traffic subscriber and type of traffic have been identified, the policies for that subscriber are enforced by the traffic flow scanning processor.

At page 3 of Office Action, Examiner erroneously asserts that Maher teaches, *the network interface component comprising: a network traffic analyzer (NTA) component that analyzes network data and diagnoses network related data problems,* with respect to independent claim 1. The cited portion of reference (Maher) provides for service providers entering into service level agreements with their customers. The service level agreements are monitored and statistics are collected to determine if the service provider met, failed to meet or exceeded the service levels set out in the service level agreements (*See*, Paragraph [0022]). Service provider network apparatus includes a traffic flow scanning processor, which includes a header processor and a payload analyzer. The payload analyzer scans the contents of data packets received from the header processor, particularly the payload contents of the data packets. The payload analyzer compares the contents of all data packets against a database of known signatures and if the contents of a data packet match a known signature, an action associated with that signature is taken (*See*, Paragraphs [0031] & [0040]). Hence, Maher provides for associating a data packet in traffic flow with a particular subscriber, identifying type and nature of the network traffic related to the particular subscriber and enforcing policies for that subscriber according to service level agreement between the service provider and the subscriber. However, Maher does not teach or suggest a network traffic analyzer component that analyzes network data *and diagnoses network related data problems*. Further, the payload analyzer is embedded within the network apparatus of service provider only and hence system disclosed by Maher, requires *use of a separate hardware or separate computer* such as service provider's network apparatus. However, Maher does not contemplate embedding the network traffic analyzer component into the interface of a networked device or devices which are routinely connected to network. The claimed subject matter facilitates eliminating the need for a separate dedicated network traffic analyzer such as payload analyzer in the network apparatus of service provider, for most routine applications. The use of a dedicated network traffic analyzer is time consuming, inefficient and expensive for the network user. Furthermore, the presence of an additional device not normally a part of the network alters the network configuration and the loading on the bus. The addition of an additional device can mask the problem and/or create a new problem. The claimed subject matter provides for diagnosing the network problem without

the need to add dedicated support equipment which alters the configuration of the network system and alters the load on the bus.

At page 5 of Office Action, the Examiner erroneously asserts that Maher teaches, the network traffic analyzer filter component comprising a data acquisition component that facilitates a filter *and analysis of network related data problems*, with respect to dependent claim 13. The cited portion of reference (Maher) talks about need of an intelligent and content aware network that is able to identify and filter out security problems such as email worms, viruses, denial of service attacks and making those transparent to end users (*See*, Paragraph [0024]). The network device, disclosed by Maher, is operable to determine if a data packet belongs to a registered customer with a set of programmed policies residing on the network device. The network device is operable to scan the contents of each data packets and determine the type of content, such as email, web surfing, video and file transfer. Based upon the contents, the network device handles the data packet for enforcing service level agreements (*See*, Paragraph [0053]). Hence, Maher discusses need of identifying and filtering out *security related problems only* and provides a network device which can scan each data packet and determine if the data packet belongs to a registered customer with a set of programmed policies residing on the network. However, Maher does not contemplate the network traffic analyzer filter component that facilitates a filter and analysis of *network related data problems*, as recited in dependent claim 13 *and diagnosing network related data problems*, as recited in independent claim 1.

At page 6 of the Office Action, the Examiner again erroneously asserts that Maher teaches, *a method for allocating network traffic analysis tasks to networked devices comprising: activating respective monitoring components embedded into network interface of a plurality of devices of a network*, with respect to independent claim 19. The cited portion of reference (Maher) provides for network apparatus including a payload analyzer. The payload analyzer includes three separate engines, queue engine, context engine and payload scanning engine. Context engine works with queue engine to select a new context when a context has finished processing and been transmitted out of payload analyzer. Next free context identifies the next block of a data packet to process. Only one data packet can be active at one time because payload analyzer must scan data packets in order (*See*, Paragraph [0044]). After a data packet has been associated with a subscriber and traffic type has been identified, the associated queue is checked for available bandwidth as defined in subscriber's policies and profile. Available

bandwidth is determined by comparing the maximum bandwidth, as defined in the subscriber's policies, minus the used bandwidth (*See*, Paragraph [0054]). Hence, Maher provides for only *one* network apparatus comprising a payload analyzer for scanning payload information and related context associated with each data packet. The network apparatus belongs to a service provider and only that network apparatus includes an analyzer or monitoring component. However, Maher does not contemplate allocating network traffic analysis tasks to *networked devices* and *activating respective monitoring components embedded into network interface* ***of a plurality of devices of a network***. Further, Maher provides for calculating bandwidth for a data packet associated with a subscriber by subtracting used bandwidth by the subscriber from the available bandwidth defined in the subscriber's policies. However, Maher does not contemplate determining *which devices* have greatest available resources among the networked devices based at least in part on the resource utilization data and allocating network traffic analysis tasks based at least in part on the available resources.

Accordingly, applicants' representative respectfully submits that Maher fails to teach or suggest all limitations of applicants' claimed subject matter as recited in independent claims 1, 18, 19, 20 and 21 (and claims that depend there from). Consequently, this rejection should be withdrawn.

II. New Claims 24-27

Newly added claims 24-27 emphasize novel aspects of the invention discussed *supra* in connection with claims 1, 18, 19, 20 and 21. Support for these claims can be found in the specification as filed at page 13, lines 5-20, Fig. 6 and page 14, lines 21-30, Fig. 8. Accordingly, these claims are patentably distinct over the art of record for at least the same reasons as are claims 1, 18, 19, 20 and 21.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP296US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731